REMARKS

Claims 1-28 were presented for examination.

Claims 1-28 were rejected.

Reconsideration of this application and allowance of all pending claims, claims 1-28, are hereby respectfully requested.

Claims 1-28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Smith in view of Vazana. This rejection is respectfully traversed.

Applicants' claims generally concern escrow encryption, where an information package destined for an addressee is encrypted with an escrow encryption key in response to the addressee not having a public key. In contrast, in Smith, items are encrypted and an addressee may not have a public key, but items are NOT encrypted in response to an addressee not having a public key. Vazana generally does not concern encryption and does not cure the fundamental shortcomings of Smith. Thus, Applicants respectfully submit that neither Smith nor Vazana, either alone or in combination, teach or suggest the claimed invention.

In more detail, claim 1 concerns a method for securely transmitting an information package to an addressee. The method determines whether the addressee has a public key and "in response to the addressee not having a public key: encrypt[s] the package with an escrow encryption key" (emphasis added). Note that the package is encrypted with an escrow encryption key in response to the addressee not having a public key.

As an example, consider FIG. 3:

> "A determination 306 is made whether the addressee's key was found in the directory 112. If the key was found, the package 10 is encrypted 308 by the encryption module 114 using the addressee's public key and is sent to the server

system 104, where it is stored 310 as a "regular" package. The term "regular" is used to distinguish the package 10 from one being stored in "escrow" for an addressee who does not yet have a public key. In one embodiment, a separate storage area (not shown) in the server system 104 is provided for regular packages." P. 14, ll. 11-18.

"[I]f the addressee's public key was not found in the directory 112, the escrow key manager 116 issues 324, for the package 10, an escrow encryption key and an escrow decryption key. The escrow encryption key is used for encrypting the package 10 prior to being stored in escrow, and the escrow decryption key is used for decrypting the package 10.

The escrow encryption/decryption keys should not be confused with the new public and private keys issued to the addressee, as described in step 336." P. 17, ll. 3-8.

This feature is beneficial, because, as pointed out in the application, "a sender is not required to know the addressee's public key before a package (10) is sent. Indeed, the addressee is not required to have a public key before the package (10) is sent." P. 5, ll. 20-21.

This claimed feature is not shown or suggested by any of the cited references. In Smith, there is no equivalent to an escrow encryption key and there is no encryption by an escrow encryption key in response to an addressee not having a public key.

The Office Action asserts that Smith's secret key 65 is the equivalent to claim 1's escrow encryption key. This is not the case because Smith's secret key 65 is not used to encrypt information in response to the addressee not having a public key, as recited in claim 1. Rather, the secret key 65 is used for a sort of double encryption. As an alternative to encrypting information using the addressee's public key, the information is encrypted using the secret key (e.g., a symmetric key) and the secret key is then encrypted using the addressee's public key. Encryption by the secret key occurs regardless of whether the addressee has a public key. As stated in col. 4, l. 64 – et seq., "the sender encrypts the document 40 using a secret key. . . . The sender then contacts a Delivery Server 45 to query 50 the public key associated with the intended

recipient." The secret key is used to encrypt the document before the system even knows whether the recipient has a public key. Therefore, the encryption cannot be in response to the addressee not having a public key, as recited in claim 1.

The other cited reference Vazana generally concerns electronic mail, not encryption. The Office Action relies on Vazana for the alleged disclosure of other elements in the claims. Regardless of whether this is the case, Vazana does not disclose or suggest any cure to the fundamental shortcoming of Smith. Specifically, Vazana does not teach or suggest an escrow encryption key or the encryption of an information package with an escrow encryption key in response to the addressee not having a public key. Hence, the combination of Smith and Vazana also fails to disclose or suggest the method of independent claim 1 (and its dependent claims).

The remaining independent claims 12, 17 and 28 have similar limitations, requiring either escrow encryption keys or the exact language set forth in claim 1. Thus, for the same reasons as given above, Applicants respectfully submit that these claims and their dependent claims are also patentably distinct over the cited art.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

Closing

Applicants believe that the application is in condition for allowance of all claims herein, claims 1-28, and therefore an early Notice of Allowance is respectfully requested. If the Examiner believes that for any reason direct contact with Applicants' attorney would help advance the prosecution of this case to finality, the Examiner is invited to telephone the undersigned at the number given below.

Respectfully submitted,

ENG-WHATT TOH et al.

Date: July 14, 2003

By: _____

Michael W. Farn
Attorney for Applicants
Registration No. 41,015

Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
(650) 335-7823 (Tel)
(650) 938-5200 (Fax)